UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE CAPITAL ONE CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 1:19-md-2915 (AJT/JFA)
This Document Relates ONLY to the following Case: MARCUS MINSKY, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, RICHARD FAIRBANK, and R. SCOTT BLACKLEY, Defendants.	Case No. 1:19-cv-1472 (AJT)

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION TO DISMISS THE CLASS ACTION COMPLAINT

TROUTMAN SANDERS LLP
Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
1001 Haxall Point
Richmond, VA 23219
Tel.: (804) 697-1200
Fax: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
401 9th Street, NW, Suite 1000
Washington, DC 20004
Tel.: (703) 734-4334
Fax: (703) 734-4340
mary.zinsner@troutman.com

KING & SPALDING LLP
David L. Balser (*pro hac vice*)
Michael R. Smith (*pro hac vice* pending)
Kevin J. O'Brien (VSB No. 78886)
Benjamin Lee (*pro hac vice* pending)
Peter Starr (*pro hac vice*)
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
mrsmith@kslaw.com
kobrien@kslaw.com
blee@kslaw.com
pstarr@kslaw.com

Counsel for Defendants Capital One Financial Corporation, Richard Fairbank, and R. Scott Blackley

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

On July 29, 2019, Capital One Financial Corporation ("Capital One" or the "Company") announced that it had been targeted in a criminal cyber-attack involving certain personal information of approximately 106 million Capital One credit card customers and persons who had applied for credit card products (the "Cyber Incident"). After this announcement, the Company's stock price temporarily declined by less than 6% (but has since more than fully recovered). This lawsuit followed, accusing the Company and senior management of securities fraud and seeking recovery of monetary damages based on the short-lived decline in Capital One's share price.

According to a certification filed with his Complaint,[1] Plaintiff Marcus Minsky acquired *fewer than five shares* of Capital One common stock during the alleged class period at prices ranging from $95.82/share to $99.04/share—all of which are below the trading price of $101.38/share at which Capital One's common stock closed on December 6, 2019. Based on conclusory and hindsight allegations that the Cyber Incident showed Capital One "did not maintain robust information security protections," the Complaint alleges that general statements about Capital One's information security efforts that appeared in the Company's SEC filings or on its corporate website defrauded investors. The Complaint asserts a claim that Defendants face liability under Section 10(b) of the Securities Exchange Act of 1934 and that Capital One's Chief Executive Officer and Chief Financial Officer also face liability under Section 20(a) of the Exchange Act as "controlling persons" of Capital One.

For reasons explained more fully below, Plaintiff's Complaint falls far short of satisfying the exacting pleading standards imposed by the Private Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u-4 *et seq*. (the "PSLRA") and therefore must be dismissed. *First*, Plaintiff fails to

[1] *See* Case 1:19-cv-01472-AJT-JFA, Document 1-1.

plead at all—let alone with particularity—facts showing that any of the challenged cybersecurity statements are false or misleading, as required by the PSLRA. Instead, Plaintiff simply points to the fact that the Cyber Incident occurred as support for allegations that Capital One failed to implement adequate data security safeguards. So reflexive is this effort that Plaintiff inexplicably challenges statements in Capital One 10-Ks warning of increased costs and reputational damage in the event of the theft, loss or misuse of information, including as a result of a cyber-attack. These conclusory allegations come nowhere close to satisfying the PSLRA's heightened standards for adequately pleading actionable misleading statements. *Second*, Plaintiff's allegations challenging Capital One's Online & Mobile Privacy Statement (the "Website Privacy Statement"), which is alleged to have appeared on Capital One's website, fail to state a claim for relief because the Website Privacy Statement was neither directed to *investors* nor "reasonably calculated to influence the investing public," and therefore is not a statement made "in connection with" the purchase or sale of securities upon which Section 10(b) liability can be predicated. 15 U.S.C. § 78j(b). *Third*, Plaintiff fails to plead particular facts raising the required *strong* inference of scienter as to any Defendant. Plaintiff's conclusory allegations that Defendants had "knowledge" of the purported falsity of their statements does not satisfy this exacting standard. *Fourth*, Plaintiff fails to adequately plead economic loss resulting from the alleged misstatements, as opposed to the adverse news of the Cyber Incident. *Finally*, Plaintiff's Section 20(a) claim must be dismissed because Plaintiff has not adequately pled a primary violation of Section 10(b).

II. SUMMARY OF PLAINTIFF'S ALLEGATIONS

A. The Parties

Defendant Capital One is a publicly-traded company whose common stock is listed on the New York Stock Exchange. Compl. ¶ 7. Capital One operates as the bank holding company for Capital One Bank (USA), National Association and Capital One, National Association. *Id.*

Capital One provides various financial products and services in the United States, United Kingdom, and Canada. *Id.* The Company is incorporated in Delaware and headquartered in Virginia. *Id.* Defendant Richard Fairbank is Capital One's Founder, Board Chairman, Chief Executive Officer and President. *Id.* ¶ 8. Defendant R. Scott Blackley is Capital One's Chief Financial Officer. *Id*. ¶ 9.

Plaintiff Minsky claims to have purchased fewer than five shares of Capital One common stock at prices ranging from $95.82/share to $99.04/share in transactions executed on February 23 and 28, 2018 and March 31, 2018. *See* Case 1:19-cv-01472-AJT-JFA, Document 1-1.[2]

B. The Cyber Incident

On July 29, 2019, Capital One issued a press release reporting "unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers." Compl. ¶ 21. The Company stated, based on analysis undertaken to date, that the event appeared to have affected approximately 100 million individuals in the United States and approximately 6 million in Canada, that no credit card account numbers or log-in credentials were compromised, and that over 99 percent of Social Security numbers were not compromised. *Id.* The release also stated that the Company had immediately fixed the configuration vulnerability that had been exploited and promptly began working with federal law enforcement. *Id.* The Federal Bureau of Investigation

[2] On the December 2, 2019 PSLRA deadline for filing motions seeking appointment of a lead plaintiff and lead counsel for this securities action, the same lead firm that filed Mr. Minsky's Complaint filed a motion on behalf of a different shareholder, Edward Shamoon, requesting that Mr. Shamoon be appointed as lead plaintiff for the securities action and that they be approved as lead counsel for the securities action. *See* Document 216. A Certification and "Loss Chart" filed with Mr. Shamoon's motion states that he purchased 250 shares of Capital One common stock during the alleged class period and claims to have suffered $2,319.49 in losses on his investment. *See* Documents 216-3 & 216-4. Mr. Shamoon's was the only motion filed seeking appointment as lead plaintiff and lead counsel for the securities action.

arrested the individual responsible for the unauthorized access, and to date, Capital One is aware of no evidence that the appropriated information was used for fraudulent purposes or further disseminated by that individual. *Id.*

C. Plaintiff's Claims and the Challenged Statements

Plaintiff challenges four basic categories of statements. *First*, Plaintiff challenges an excerpt from Capital One's Website Privacy Statement, which Plaintiff alleges was "last updated May 1, 2014 and [was] found on [Capital One's] website throughout the Class Period," stating:

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information***. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices.***

Id. ¶ 15 (Emphasis added). *Second*, Plaintiff alleges that Capital One's Annual Reports on SEC Form 10-K for the years ended December 31, 2017 (the "2017 10-K") and December 31, 2018 (the "2018 10-K") included statements (the "Data Security Statements") that:

> ***We safeguard our customers' and our own information and technology, implement backup and recovery systems, and generally require the same of our third-party service providers. We take measures that mitigate against known attacks and use internal and external resources to scan for vulnerabilities in platforms, systems, and applications necessary for delivering Capital One products and services.***

Compl. ¶¶ 17 & 19. *Third*, Plaintiff bizarrely challenges Risk-Factor statements in the 2017 and 2018 10-Ks (the "Cyber-Risk Warnings") clearly warning that:

> Although we believe we have a robust suite of authentication and layered information security controls, including our cyber threat analytics, data encryption and tokenization technologies, anti-malware defenses and vulnerability management program, *any one or combination of these controls could fail to detect, mitigate or remediate these risks in a timely manner*.

Id. (emphasis added). *Finally*, Plaintiff challenges "certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX")" signed by Defendants Fairbank and Blackley "attesting to the accuracy of

financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud" that were included with the 2017 and 2018 10-Ks (the "SOX Certifications"). *Id.* ¶ 16.

Plaintiff alleges that all of the above challenged statements were false or misleading or because "(1) [Capital One] did not maintain robust information security protections, and its protection did not shield personal information against security breaches; (2) such deficiencies heightened the Company's exposure to a cyber-attack; and (3) as a result, Capital One's public statements were materially false and misleading at all relevant times." *Id*. ¶ 20.

III. LEGAL STANDARDS

To state a claim under Section 10(b) and SEC Rule 10b-5, Plaintiff must allege and ultimately prove six elements: (1) a material misrepresentation or omission of material fact; (2) scienter; (3) a connection with the purchase or sale of a security; (4) reliance; (5) economic loss; and (6) loss causation. *See Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 341-42 (2005).

Plaintiff's claims are subject to the heightened pleading standards of Rule 9(b) and the PSLRA. Rule 9(b) provides that in "alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b). Rule 9(b) "encapsulates the goal of sorting out at an early stage 'strike suits' in the securities field." *See Teachers' Ret. Sys. of La. v. Hunter*, 477 F.3d 162, 171 (4th Cir. 2007) (citation omitted). In addition to the pleading requirements of Rule 9(b), this case is also subject to the "exacting pleading requirements of the PSLRA," through which "Congress charged courts to be vigilant in preventing meritless securities fraud claims from reaching the discovery phase of litigation." *Cozzarelli v. Inspire Pharms., Inc.*, 549 F.3d 618, 623 (4th Cir. 2008). In enacting the PSLRA, Congress determined it

was necessary to raise the bar even higher than Rule 9(b) in the context of securities fraud. *See Maguire Fin., LP v. PowerSecure Int'l, Inc*., 876 F.3d 541, 546 (4th Cir. 2017).

The PSLRA requires that Plaintiff "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, … state with particularity all facts on which that belief is formed." 15 U.S.C. § 78u-4(b)(1). Additionally, the PSLRA requires that Plaintiff "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." *Id*. § 78u-4(b)(2)(A). The "required state of mind" is scienter, defined to mean "a mental state embracing intent to deceive, manipulate, or defraud." *See Tellabs, Inc. v. Makor Issues & Rights, Ltd*., 551 U.S. 308, 319 (2007) (internal quotation marks and citation omitted). A "strong inference" of scienter is one that is "more than merely plausible or reasonable—it must be cogent and at least as compelling as any opposing inference of nonfraudulent intent." *Id*. at 314. The PSLRA also requires Plaintiff to plead "economic loss" that is caused by the alleged misrepresentations, rather than the multitude of other factors that can move a stock's price. *Dura*, 544 U.S. at 345. The Fourth Circuit Court of Appeals has held that the claim element of loss causation must be pled "with sufficient specificity to enable the court to evaluate whether the necessary causal link exists," *Hunter*, 477 F.3d at 186, and confirmed that this standard is "consonant with Fed. R. Civ. P. 9(b)'s requirement that averments of fraud be pled with particularity." *Katyle v. Penn Nat'l Gaming, Inc*., 637 F.3d 462, 471 (4th Cir. 2011), *cert. denied*, 565 U.S. 825 (2011).

IV. ARGUMENT

A. Plaintiff Fails To Plead Falsity At All, Let Alone With Particularity.

Plaintiff's claims rest entirely upon the conclusory and unsupported assertion that the challenged statements were false simply because the Company was the victim of an unauthorized data theft. The Complaint lacks the required allegations of particular facts showing that the challenged statements were false or misleading when made and therefore must be dismissed for failure to adequately plead a claim for relief. *See* 15 U.S.C. § 78u-4(b)(1); *see also* FED. R. CIV. P. 9(b).

1. Conclusory Allegations That Capital One's Security Protections Were Not "Robust" And Did Not Prevent The Cyber Incident Fail To Show That Any Of The Challenged Statements Were False.

The crux of Plaintiff's allegations is that the challenged statements were false or misleading because "the Company did not maintain robust information security protections" and "its protection did not shield personal information against security breaches." Compl. ¶ 20. These conclusory allegations fall far short of satisfying the PSLRA's heightened standards for pleading falsity for several reasons.

First, the fact that the Cyber Incident occurred does not render the challenged statements false or misleading (nor does it even establish that Capital One lacked robust security measures). In a similar case, another federal court rejected substantively identical securities fraud claims predicated on allegations that the failure to implement adequate cybersecurity measures resulted in the theft of sensitive consumer data. *See In re Heartland Payment Sys., Inc. Sec. Litig.*, Civ. No. 09-1043, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009). In *Heartland*, the plaintiffs alleged that the defendant payment processing company misrepresented the state of its data security prior to a cyber-attack that resulted in the theft of 130 million credit and debit card numbers, contending that the breach proved that those statements had been false or misleading. *Id.* at *4-6. The court

dismissed the plaintiff's claims, however, holding that "[t]he fact that a company has suffered a security breach does not demonstrate that the company did not 'place significant emphasis on maintaining a high level of security.'" *Id.* at *5. Specifically, the court held that the breach did not render the defendants' aspirational statements about security false or misleading, finding that it was more plausible that "Heartland did place a high emphasis on security but that the Company's security systems were nonetheless overcome." *Id*. ("[T]he alleged facts are more plausibly explained by lawful behavior than illegal deception").

Plaintiff's allegations are far weaker and less particular than those in *Heartland*. *Compare, e.g., Heartland*, 2009 WL 4798148 at *5-6 (addressing statements that Heartland "place[d] significant emphasis on maintaining a high level of security" and maintained a network configuration that "provides multiple layers of security to isolate our databases from unauthorized access"), *with, e.g.*, Compl. ¶ 15 ("[W]e make your safety and security a top priority . . . ."); *id.* ¶ 17 ("We safeguard our customers' and our own information and technology, implement backup and recovery systems . . . ."); *id.* ("We take measures that mitigate against known attacks and use internal and external resources to scan for vulnerabilities . . . ."). As with the corporate defendant in *Heartland*, the fact that Capital One suffered a criminal cyber-attack does not render false its prior statements about commitment to cybersecurity, efforts to protect sensitive information, and measures taken to mitigate related risks. *See Heartland*, 2009 WL 4798148, at *5-6.

Second, even if Plaintiff had pled particular facts supporting their allegations that Capital One lacked robust information security protections (and he has not) such allegations would not suffice to plead the falsity of statements that Capital One "protect[ed]" information in its custody, "safeguard[ed]" information and technology, took measures "that mitigate against known attacks," and "use[d] internal and external resources to scan for vulnerabilities." *Id.* ¶¶ 15, 17, 19. Instead,

Plaintiff merely second-guesses the extent or efficacy of those efforts. Absent particularized allegations that Capital One did not in fact have a data security system, hindsight allegations that the Company's efforts did not succeed in preventing the Cyber Incident do not support a claim for securities fraud. *See Ong v. Chipotle Mexican Grill, Inc.* ("*Chipotle II*"), 294 F. Supp. 3d 199, 232 (S.D.N.Y. 2018) (holding that allegations that did not "conflict with Defendants' statements regarding the . . . programs and procedures that Chipotle had in place, but merely quibble[d] with [the] execution of those programs and procedures," failed to adequately plead the statements' falsity); *see also Howard v. Arconic Inc.*, 395 F. Supp. 3d 516, 547 (W.D. Pa. 2019) ("Arconic's general statements about its values, workplace safety, and ethics—which read like mission statements rather than guarantees—were not rendered misleading by product safety issues related to Reynobond PE's ultimate use."). Likewise, Plaintiff has failed to show that the challenged statements referring to Capital One's general commitment to data security were false or misleading. *See, e.g.*, Compl. ¶ 15 (safety and security are a "top priority" and Capital One is "committed to protecting your personal and financial information."). Challenges to the efficacy of Capital One's security systems do not establish that Capital One was not committed to data security. *See Heartland*, 2009 WL 4798148, at *5.

Instead, such allegations at best seek to dress up claims of corporate mismanagement as securities fraud and thus fail to state a claim under Section 10(b). Indeed, as the Supreme Court held forty years ago, "Congress by [enacting] § 10(b) did not seek to regulate [conduct] which constitute[s] no more than internal corporate mismanagement." *See Santa Fe Indus. v. Green*, 430 U.S. 462, 479-80 (1977) (internal quotation marks omitted). Allegations that Defendants should have implemented different or better security measures to protect data are, at most, allegations of "mismanagement," for which the securities laws do not provide a remedy. *See id*. Further, merely

alleging a failure to disclose possible mismanagement and operational issues does not state a claim under Section 10(b). *See Cutsforth v. Renschler*, 235 F. Supp. 2d 1216, 1242-44 (M.D. Fla. 2002) (applying *Santa Fe* and dismissing claims similarly based on alleged failure to disclose "severe problems" with computer systems and other operational problems).

For all of these reasons, Plaintiff's allegations that Capital One "did not maintain robust information security protections," "its protection did not shield personal information against security breaches," and "such deficiencies heightened the Company's exposure to a cyber-attack" (Compl. ¶ 20) fall far short of satisfying the PSLRA's requirement to plead particular facts demonstrating that the challenged statements were false or misleading.

2. Plaintiff Has Not Pled Falsity Of The SOX Certifications.

Plaintiff's claims challenging the SOX Certifications also must be dismissed because Plaintiff fails to plead any facts suggesting that those statements were false and misleading. As alleged in the Complaint, the SOX Certifications address "the accuracy of [Capital One's] ***financial reporting***." Compl. ¶¶ 16, 18 (emphasis added). The Complaint does not include any allegations at all, much less allegations of particular facts, suggesting that Capital One's ***financial reporting*** was in any way inaccurate or that the Company lacked internal controls of the type described by the SOX certifications. Accordingly, Plaintiff's claims challenging the SOX Certifications must be dismissed. *See, e.g.*, *In re Banco Bradesco S.A. Sec. Litig.*, 277 F. Supp. 3d 600, 648-49 (S.D.N.Y. 2017) (dismissing claims challenging certifications about financial reporting controls where plaintiff failed to allege any failure in financial reporting (*e.g.*, a need to restate published financial results)) (citing cases).

3. Plaintiff Has Not Pled That The Cyber-Risk Warnings Were Misleading.

Plaintiff also fails to adequately plead the falsity of the Cyber-Risk Warnings, which in addition to warning that Capital One could suffer a significant and damaging cyber-attack stated that "we believe we have a robust suite of authentication and layered information security controls, including our cyber threat analytics, data encryption and tokenization technologies, anti-malware defenses and vulnerability management program." Compl. ¶¶ 17, 19. Such statements of belief or opinion are not actionable unless the plaintiff pleads sufficient facts to establish that the speaker did not actually hold the stated belief at the time it was expressed. *See Nolte v. Capital One Fin. Corp.*, 390 F.3d 311, 315 (4th Cir. 2004) (holding that to plead an opinion is a false statement, the complaint "must allege that the opinion expressed was different from the opinion actually held by the speaker"); *see also Longman v. Food Lion, Inc*., 197 F.3d 675, 683 (4th Cir. 1999) ("Opinions c[an] be false and factual if the [speakers] did not believe what they said they believed"). Plaintiff has not alleged any particularized facts showing that Defendants did not genuinely believe Capital One's information security measures were robust, as stated. Nor does Plaintiff plead facts demonstrating that Capital One did not have in place the various security measures referenced in this opinion statement. Plaintiff's claim challenging the Cyber-Risk Warnings therefore fails as a matter of law.

B. The Website Privacy Statement Was Not Made "In Connection With" The Purchase Or Sale Of Securities And, Thus, Is Not Actionable.

In addition to the lack of supporting fact allegations establishing that the Website Privacy Statement was in any way false or misleading (*see* Section IV.A.1.), Plaintiff's claim challenging this statement also fails for the additional and independent reason that the statement does not qualify as one made "in connection with" the purchase or sale of a security, as required to give rise

to a claim under Section 10. *See* 15 U.S.C. § 78j(b); *see also SEC v. Tex. Gulf Sulphur Co.*, 401 F.2d 833, 858-64 (2d Cir. 1968) (discussing the "in connection with requirement").

In order to satisfy the "in connection with" requirement, a statement must have been made "in a manner reasonably calculated to influence the investing public." *Tex. Gulf Sulphur*, 401 F.2d at 862; *accord McGann v. Ernst & Young*, 102 F.3d 390, 397 (9th Cir. 1996). The Website Privacy Statement, which is not alleged to have been included in any SEC filing or other communication directed to *investors*, but instead is alleged to have been a *consumer-directed* statement appearing on Capital One's website, does not meet this standard. *See In re LifeLock, Inc. Sec. Litig.*, 690 Fed. App'x 947, 954 (9th Cir. 2017) (finding that alleged statements made in advertisements "might have some probative value in an action based on consumer protection laws," but "have none in a case alleging investor fraud"); *cf. SEC v. Rana Research, Inc*., 8 F.3d 1358, 1362 (9th Cir. 1993) (citing cases showing that statements actionable under Section 10(b) typically include those published in company press releases, annual and quarterly reports, analyst reports, proxy statements, and other SEC filings). Because it was not made "in connection with the purchase or sale of any security," the Website Privacy Statement is not actionable under Section 10(b). 15 U.S.C. § 78j(b).[3]

C. Plaintiff Fails to Allege Particularized Facts Giving Rise To A Strong Inference of Scienter.

Plaintiff's Complaint also must be dismissed because it fails to meet the PSLRA's heightened standards for pleading scienter. *See* 15 U.S.C. § 78u-4(b)(2)(A). Plaintiff relies entirely on conclusory allegations that Defendants had knowledge of or access to undisclosed

[3] The Complaint fails to allege that the Individual Defendants made or approved the Website Privacy Statement, providing an independent basis for their dismissal with respect to this statement. *See Janus Capital Group, Inc. v. First Deriv. Traders*, 564 U.S. 135, 142 (2011) ("For purposes of Rule 10b–5, the maker of a statement is the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it.").

information regarding the Company's cybersecurity by virtue of their positions in the Company. Such allegations are insufficient under the PSLRA, which instead requires Plaintiff to plead *particularized facts* giving rise to a strong inference that Defendants acted with scienter. *PowerSecure*, 876 F.3d at 548 (quoting 15 U.S.C. § 78u-4(b)(2)). Plaintiff must plead such particular facts supporting a strong inference of scienter as to each defendant with respect to each violation. *See Hunter*, 477 F.3d at 184. And "if the defendant is a corporation, the plaintiff must allege facts that support a strong inference of scienter with respect to at least one authorized agent of the corporation, since corporate liability derives from the actions of its agents." *Id.* Plaintiff's Complaint fails to satisfy these tests.

1. Plaintiff Fails To Raise A Strong Inference Of Actual Knowledge Or Severe Recklessness.

Plaintiff relies exclusively on two categories of conclusory allegations in favor of scienter: (i) that Defendants had "knowledge" of the falsity of their statements, and (ii) that they had access to information demonstrating this falsity by virtue of their positions within the Company. *See, e.g.*, Compl. ¶ 11 (defendants were "aware of or recklessly disregarded the fact that the false and misleading statements were being issued"); *id.* ("Each of the Individual Defendants . . . was privy to confidential proprietary information concerning the Company and its business and operations . . . ."); *id.* ¶ 38 ("Defendants acted with scienter in that they knew that the public documents and statements issued . . were materially false . . . .") ; *id.* ¶ 39 ("Individual Defendants . . . intended to deceive Plaintiff . . . or, in the alternative, acted with reckless disregard . . . ."). These allegations fall far short of meeting the PSLRA's exacting requirements.

First, Plaintiff alleges that Defendants "intended to deceive" and "knew that the public documents and statements" were false or misleading. Compl. ¶¶ 38, 39. However, such conclusory assertions fail to meet the PSLRA's heightened pleading standards for scienter. *See In*

re Genworth Fin. Inc. Sec. Litig., 103 F. Supp. 3d 759, 783 (E.D. Va. 2015) ("Adding the words 'knowingly' or 'recklessly' to a factual statement is insufficient pleading." (internal quotations omitted)); *Smith v. Circuit City Stores, Inc.*, 286 F. Supp. 2d 707, 714-15 (E.D. Va. 2003) ("Pleadings that couple a factual statement with a conclusory allegation of fraudulent intent are too broad and conclusory under the Reform Act." (internal quotations omitted)). Plaintiff's barebones allegations that Defendants acted with "knowledge" fail to satisfy the PSLRA's particularity requirements.

Second, Plaintiff cites the Individual Defendants' positions in the company and access to material non-public information in support of a finding of scienter. *See* Compl. ¶¶ 11, 38, 39. However, absent other particularized allegations, such speculative and generic pleading fails to establish a strong inference of scienter. "Guesswork of this kind, based on the position of the Defendants is insufficient under the Reform Act." *Circuit City*, 286 F. Supp. 2d at 715 (citing *In re First Union Corp. Sec. Litig.*, 128 F. Supp. 2d 871, 888 (W.D.N.C. 2001)). These allegations are not supported by any particularly pled facts showing that Defendants, because of their positions in the Company, received specific information contradicting their public statements about Capital One's cybersecurity. As such, they fail to satisfy the stringent standards of the PSLRA. *See Circuit City*, 286 F. Supp. 2d at 715.

Essentially, Plaintiff relies on the occurrence of the Cyber Incident itself, and nothing more, to presume both that the public statements were false and that Defendants knew they were false when made. But these allegations show no such thing, and they are insufficient under the PSLRA. *See, e.g., Heartland*, 2009 WL 4798148, at *7-8 (finding scienter not adequately pled where allegations failed to show defendants believed data security measures were deficient when speaking about them); *see also Plymouth Cnty. Ret. Ass'n v. Primo Water Corp.*, 966 F. Supp. 2d

525, 547 (M.D.N.C.) (rejecting hindsight allegations); *Hunter*, 477 F.3d at 181 (similar). Plaintiff does not plead any facts suggesting that, at the times the challenged statements were made, Defendants knew of or recklessly disregarded contrary or conflicting information. Furthermore, there are no allegations of insider trading or other improper motive by Defendants. "While insider trading may . . . support an inference of scienter . . ., it only will do so if the timing and amount of the sale(s) are 'unusual or suspicious.'" *In re PEC Sols., Inc. Sec. Litig.*, 418 F.3d 379, 390 (4th Cir. 2005). This failure to allege an improper personal motive weighs against a finding of scienter. *See Cozzarelli*, 549 F.3d at 626 (lack of unlawful intent weighs against finding of scienter).

2. The More Compelling Inference Is That Defendants Believed The Challenged Statements.

As discussed above, Plaintiff's theory of scienter rests on a combination of hindsight and conclusory speculation. Essentially, Plaintiff claims—based on the occurrence of the Cyber Incident itself—that Defendants knew about supposed vulnerabilities in Capital One's data security systems but nonetheless issued statements regarding the strength and importance of these systems, statements which Plaintiff alleges, in conclusory fashion, were fraudulent. In weighing scienter, "[a] court must compare the malicious and innocent inferences cognizable from the facts pled in the complaint, and only allow the complaint to survive a motion to dismiss if the malicious inference is at least as compelling as any opposing innocent inference." *Yates v. Mun. Mortgage & Equity, LLC*, 744 F.3d 874, 885 (4th Cir. 2014). Because Plaintiff's conclusory and circumstantial allegations are far outweighed by a much more compelling inference of non-fraudulent intent, the complaint should be dismissed. *See Tellabs*, 551 U.S. at 324

The more compelling inference is that, when the challenged statements were made, Defendants genuinely believed that Capital One's data security measures were reasonably and appropriately designed to protect sensitive information in its custody and that the statements were

accurate. As even the Federal Trade Commission has recognized, "there is no[] such thing as perfect security." *See* "Data Security: Why It's Important, What the FTC is Doing About It," March 24, 2014 Remarks by Jessica Rich, Director, Bureau of Consumer Protection, FTC, p. 4 (https://www.ftc.gov/system/files/documents/public_statements/295751/140324nclremarks.pdf). The fact that the Company suffered a criminal attack in no way raises an inference that the Defendants had knowledge that such an attack would occur or that Capital One's defenses were deficient. This inference follows naturally when considering that Plaintiff offers no allegations of *any* motivation for Defendants to make misstatements on this subject. *See Cozzarelli*, 549 F.3d at 626 ("While that sort of 'smoking-gun' allegation is not necessary to support an inference of scienter, . . . plaintiffs do have the difficult task of establishing a countervailing, cogent inference of scienter through indirect and circumstantial allegations."). Because the more compelling inference is one of non-fraudulent intent, the Complaint must be dismissed. *See Tellabs*, 551 U.S. at 324.

D. Plaintiff Has Not Sufficiently Pled Economic Loss Caused By The Alleged "Fraud."

The Complaint also must be dismissed because Plaintiff has not adequately pled that his claimed losses were caused by the alleged "fraud." To survive dismissal, a plaintiff must "allege loss causation in the complaint with sufficient specificity to enable the court to evaluate whether the necessary causal link exists." *Katyle*, 637 F.3d at 465-66. To do so, "the plaintiff must plead (1) the 'exposure' of the defendant's misrepresentation or omission, i.e., the revelation of 'new facts suggesting [that the defendant] perpetrated a fraud on the market,' and (2) that such exposure 'resulted in the decline of [the defendant's] share price." *Singer v. Reali*, 883 F.3d 425, 445 (4th Cir. 2018) (quoting *Katyle*, 637 F.3d at 473).

Where, as here, a plaintiff "has not adequately pled facts which, if proven, would show that its loss was caused by the alleged misstatements . . . as opposed to intervening events," the

Complaint fails. *Katyle*, at 471. It is not sufficient to merely allege a price decline following an announcement of negative news, as the Complaint does here. Instead, the stock price drop must follow a "corrective" disclosure that reveals the alleged fraud. Such a disclosure "must reveal to the market in some sense the fraudulent nature of the practices about which a plaintiff complains." *Id.* at 473 (quotations and citations omitted); *see also Hunter*, 477 F.3d at 187 (to allege loss causation "plaintiffs would have to allege that the market reacted to new facts . . . that revealed … previous representations to have been fraudulent.").

The Fourth Circuit recognizes two ways in which "exposure" of the fraud can be pled: (1) the corrective disclosure theory, where the defendant issues a disclosure "that 'publicly revealed for the first time' that the company perpetrated a fraud on the market," and (2) the materialization of a concealed risk theory, where "news from another source revealed the company's fraud." *Singer*, 883 F.3d at 445-46. In either instance, "the plaintiff must show that the loss caused by the alleged fraud results from the relevant truth . . . leak[ing] out." *Id*. at 446. It is unclear from Plaintiff's allegations which theory is being pursued in this case. However, the Complaint satisfies neither theory, as none of the alleged disclosures revealed any earlier misstatements.

Notably, the Fourth Circuit has explained that heightened pleading standards apply to loss causation allegations. *See Hunter*, 477 F.3d at 186. Plaintiff's conclusory loss causation allegations fail to satisfy even basic notice pleading standards under Rule 8—let alone the heightened pleading standards of Rule 9(b). Plaintiff merely alleges that the market price of the Company's securities was "artificially inflated" and that "[a]s a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Plaintiff and other Class members have suffered significant losses and damages." Compl. ¶¶ 24, 40. However, this is just a legal conclusion that falls far short of alleging particularized facts

showing that Plaintiff's purported losses were caused by any alleged fraud (or revelation thereof). For this reason alone, the Complaint fails to adequately plead loss causation and therefore must be dismissed.

Moreover, Plaintiff has failed to adequately allege either a corrective disclosure or a materialization of a concealed risk. Plaintiff alleges that Capital One's stock price dropped following the announcement of the Cyber Incident. But nowhere does the Complaint explain how that announcement revealed that any of Defendants' earlier challenged statements were false or misleading when made. The announcement did not "reveal" that the Company failed to safeguard information, or take measures to mitigate known risks. Instead, it merely announced that the Company had fallen victim to a third party's criminal act. While this negative information may have had a downward effect on the Company's stock price, it did not "reveal" a fraud. These allegations do not establish either a corrective disclosure or a materialization of a concealed risk because they do not plead that the alleged truth "leaked" out. *Singer*, 883 F.3d at 446. Accordingly, the Complaint fails to plead loss causation and must be dismissed for this reason as well.

E. The Complaint Fails To State A Claim Under Section 20(a).

Finally, Plaintiff's Section 20(a) "controlling person" liability claim also must be dismissed. Plaintiff must allege a primary violation of the securities laws to state a claim for control person liability under Section 20(a). *See Hunter*, 477 F.3d at 188. Because the Complaint fails to state a claim for violation of Section 10(b) or Rule 10b-5, the asserted Section 20(a) claim likewise fails. *See id*.

V. CONCLUSION

For the foregoing reasons, the Defendants respectfully request that the Court dismiss the Complaint with prejudice.

Respectfully submitted this 6th day of December 2019.

/s/
David L. Balser (*pro hac vice*)
Michael R. Smith (*pro hac vice* pending)
Kevin J. O'Brien (VSB No. 78886)
Benjamin Lee (*pro hac vice* pending)
Peter Starr (*pro hac vice*)
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
mrsmith@kslaw.com
kobrien@kslaw.com
blee@kslaw.com
pstarr@kslaw.com

Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
TROUTMAN SANDERS LLP
1001 Haxall Point
Richmond, VA 23219
Tel.: (804) 697-1200
Fax: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
TROUTMAN SANDERS LLP
401 9th Street, NW, Suite 1000
Washington, DC 20004
Tel.: (703) 734-4334
Fax: (703) 734-4340
mary.zinsner@troutman.com

Counsel for Defendants Capital One Financial Corporation, Richard Fairbank, and R. Scott Blackley

CERTIFICATE OF SERVICE

I hereby certify that on December 6, 2019, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/
Kevin J. O'Brien (VSB No. 78886)
KING & SPALDING LLP

Counsel for Defendants Capital One Financial Corporation, Richard Fairbank, and R. Scott Blackley